Montana Legislative History

Chapter: 201 Session L: 2017

Bill Number: 147 **House**

Checklist of Bill History

History and Final Status Sheet	x
Introduced Bill	X
Fiscal Note	X
Third Reading Bill	X
Final Version of Bill	X

House

Committee:
Judiciary
Appropriations

Hearing Date(s):

Jan. 20, 2017
(Judiciary)

Feb. 1, 2017
(Executive Action)
Feb. 8, 2017 (Appropriations)
Feb. 13, 2017 (Appropriations EA)

Conference Committee

Hearing Date(s): n/a

Conference Committee Report:

Senate

Committee: Judiciary

Hearing Date(s):
March 10, 2017
March 16, 2017 (EA)

Compiler Notes

Compiled by: sg

Date: Feb. 13, 2024

Notes:

AN ACT PROVIDING THAT A SEARCH WARRANT IS REQUIRED FOR A GOVERNMENT ENTITY TO ACCESS ANY ELECTRONIC DEVICE UNLESS INFORMED CONSENT IS OBTAINED OR A JUDICIALLY RECOGNIZED EXCEPTION TO THE WARRANT REQUIREMENT EXISTS; PROVIDING A CIVIL CAUSE OF ACTION FOR VIOLATIONS; AND PROVIDING DEFINITIONS AND EXCEPTIONS.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

Section 1. Definitions. As used in [sections 1 through 3], the following definitions apply:

(1) "Authorized user" means a person who has the permission of the owner to possess and operate the electronic device.

(2) "Electronic communication service" means a service that:

(a) provides to users the ability to send or receive electronic communications;

(b) provides to users computer storage or processing services; or

(c) acts as an intermediary in the transmission of electronic communications.

(3) "Electronic device" means a device that enables access to or use of an electronic communication service or remote computing service.

(4) "Government entity" means a state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission or an individual acting or purporting to act for or on behalf of a state or local agency.

(5) "Owner" means a person who is the legal owner of the electronic device. If the electronic device is the subject of an agreement for the conditional sale of the electronic device with the right of purchase upon performance of the conditions stated in the agreement and with an immediate right of possession vested in the person possessing the device, or in the event the electronic device is subject to a lease, contract, or other legal arrangement vesting the right of possession or control in the person possessing the electronic device, then the owner is the person in whom the right of possession or control is vested.

(6) "Remote computing service" means the provision of computer storage or processing services by

means of an electronic communications system.

(7) "Stored data" means data or records that are stored on an electronic device that contains:

(a) information revealing the identity of users of the applicable service, device, or program;

(b) information about a user's use of the applicable service, device, or program;

(c) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the user;

(d) the content of a wire communication or electronic communication sent to or by the user; or

(e) any data, documents, files, or communications stored by or on behalf of the user with the applicable service provider or on the user's electronic device.

Section 2. Electronic data privacy -- warrant required -- exceptions. (1) Except as provided in subsection (2), a government entity may not obtain the stored data of an electronic device without a search warrant issued by a court upon a finding of probable cause.

(2) A government entity may obtain the stored data of an electronic device without a search warrant:

(a) with the consent of the owner or authorized user of the electronic device;

(b) in accordance with judicially recognized exceptions to warrant requirements;

(c) if the owner has voluntarily and publicly disclosed the stored data;

(d) if the government entity, in good faith, believes that an emergency involving danger, death, or serious physical injury to a person requires immediate disclosure of communications relating to the emergency;

(e) in order to respond to the user's call for emergency services; or

(f) for any electronic devices found within the confines of an adult or youth correctional facility.

(3) Nothing in [sections 1 through 3] may be construed to limit a government entity's ability to use, maintain, or store information on its own electronic devices or to disseminate information stored on its own electronic devices.

(4) [Sections 1 through 3] do not apply to motor carrier safety or hazardous materials programs implemented by the department of transportation for purposes of complying with federal motor carrier safety regulations.

Section 3. Civil action for violation. The attorney general may apply for an injunction or commence

a civil action against any government entity to compel compliance with the terms of [sections 1 through 3].

Section 4. Codification instruction. [Sections 1 through 3] are intended to be codified as an integral part of Title 46, chapter 5, part 1, and the provisions of Title 46, chapter 5, part 1, apply to [sections 1 through 3].

- END -

I hereby certify that the within bill,

HB 0147, originated in the House.

Speaker of the House

Signed this _____ day

of _____, 2017.

Chief Clerk of the House

President of the Senate

Signed this _____ day

of _____, 2017.

HOUSE BILL NO. 147

INTRODUCED BY D. ZOLNIKOV, B. BENNETT

AN ACT PROVIDING THAT A SEARCH WARRANT IS REQUIRED FOR A GOVERNMENT ENTITY TO ACCESS ANY ELECTRONIC DEVICE UNLESS INFORMED CONSENT IS OBTAINED OR A JUDICIALLY RECOGNIZED EXCEPTION TO THE WARRANT REQUIREMENT EXISTS; PROVIDING A CIVIL CAUSE OF ACTION FOR VIOLATIONS; AND PROVIDING DEFINITIONS AND EXCEPTIONS.

HOUSE BILL NO. 147

INTRODUCED BY D. ZOLNIKOV

A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING THAT A SEARCH WARRANT IS REQUIRED FOR A GOVERNMENT ENTITY TO ACCESS ANY ELECTRONIC DEVICE UNLESS INFORMED CONSENT IS OBTAINED OR A JUDICIALLY RECOGNIZED EXCEPTION TO THE WARRANT REQUIREMENT EXISTS; PROVIDING THAT EVIDENCE OBTAINED IN VIOLATION IS NOT ADMISSIBLE; AND PROVIDING DEFINITIONS."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. **Section 1. Definitions.** As used in [sections 1 through 3], the following definitions apply:

(1) "Electronic device" means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.

(2) "Government entity" means a state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission or an individual acting or purporting to act for or on behalf of a state or local agency.

(3) "Remote computing service" means the provision of computer storage or processing services by means of an electronic communications system.

(4) "Stored data" means data or records that are stored on an electronic device that contains:

(a) information revealing the identity of users of the applicable service, device, or program;

(b) information about a user's use of the applicable service, device, or program;

(c) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the user;

(d) the content of a wire communication or electronic communication sent to or by the user; or

(e) any data, documents, files, or communications stored by or on behalf of the user with the applicable service provider or on the user's electronic device.

NEW SECTION. **Section 2. Electronic data privacy -- warrant required -- exceptions.** (1) Except

as provided in subsection (2), a government entity may not obtain the stored data of an electronic device without a search warrant issued by a court upon a finding of probable cause.

(2) A government entity may obtain the stored data of an electronic device without a search warrant:

(a) with the informed, affirmative consent of the owner or user of the electronic device;

(b) in accordance with judicially recognized exceptions to warrant requirements;

(c) if the owner has voluntarily and publicly disclosed the stored data;

(d) if there exists a possible life-threatening situation;

(e) if a government entity has possession of a lost, stolen, or otherwise unidentified device and the government entity cannot determine ownership of the device without accessing the device, then access on the part of the government entity is limited to determining ownership and a method of contacting the owner so that the device can be returned; or

(f) in order to respond to the user's call for emergency services.

(3) Nothing in [sections 1 through 3] may be construed to limit a government entity's ability to use, maintain, or store information on its own electronic devices or to disseminate information stored on its own electronic devices.

NEW SECTION. **Section 3. Admissibility of proof -- violations.** (1) Except as proof of a violation of [sections 1 through 3], evidence obtained in violation of [sections 1 through 3] is not admissible in a civil, criminal, or administrative proceeding and may not be used in any type of affidavit in an effort to obtain a search warrant or court order.

(2) The attorney general may apply for an injunction or commence a civil action against any government entity to compel compliance with the terms of [sections 1 through 3].

NEW SECTION. **Section 4. Codification instruction.** [Sections 1 through 3] are intended to be codified as an integral part of Title 46, chapter 5, part 1, and the provisions of Title 46, chapter 5, part 1, apply to [sections 1 through 3].

- END -

HOUSE BILL NO. 147

INTRODUCED BY D. ZOLNIKOV, B. BENNETT

A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING THAT A SEARCH WARRANT IS REQUIRED FOR A GOVERNMENT ENTITY TO ACCESS ANY ELECTRONIC DEVICE UNLESS INFORMED CONSENT IS OBTAINED OR A JUDICIALLY RECOGNIZED EXCEPTION TO THE WARRANT REQUIREMENT EXISTS; PROVIDING THAT EVIDENCE OBTAINED IN VIOLATION IS NOT ADMISSIBLE; AND PROVIDING DEFINITIONS AND EXCEPTIONS."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. **Section 1. Definitions.** As used in [sections 1 through 3], the following definitions apply:

(1) "Electronic device" means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.

(2) "Government entity" means a state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission or an individual acting or purporting to act for or on behalf of a state or local agency.

(3) "Remote computing service" means the provision of computer storage or processing services by means of an electronic communications system.

(4) "Stored data" means data or records that are stored on an electronic device that contains:

(a) information revealing the identity of users of the applicable service, device, or program;

(b) information about a user's use of the applicable service, device, or program;

(c) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the user;

(d) the content of a wire communication or electronic communication sent to or by the user; or

(e) any data, documents, files, or communications stored by or on behalf of the user with the applicable service provider or on the user's electronic device.

NEW SECTION. **Section 2. Electronic data privacy -- warrant required -- exceptions.** (1) Except

as provided in subsection (2), a government entity may not obtain the stored data of an electronic device without a search warrant issued by a court upon a finding of probable cause.

(2) A government entity may obtain the stored data of an electronic device without a search warrant:

(a) with the informed, affirmative consent of the owner or user of the electronic device;

(b) in accordance with judicially recognized exceptions to warrant requirements;

(c) if the owner has voluntarily and publicly disclosed the stored data;

(d) if there exists a possible life-threatening situation; OR

~~(e) if a government entity has possession of a lost, stolen, or otherwise unidentified device and the government entity cannot determine ownership of the device without accessing the device, then access on the part of the government entity is limited to determining ownership and a method of contacting the owner so that the device can be returned; or~~

~~(f)~~(E) in order to respond to the user's call for emergency services.

(3) Nothing in [sections 1 through 3] may be construed to limit a government entity's ability to use, maintain, or store information on its own electronic devices or to disseminate information stored on its own electronic devices.

(4) [SECTIONS 1 THROUGH 3] DO NOT APPLY TO MOTOR CARRIER SAFETY OR HAZARDOUS MATERIALS PROGRAMS IMPLEMENTED BY THE DEPARTMENT OF TRANSPORTATION FOR PURPOSES OF COMPLYING WITH FEDERAL MOTOR CARRIER SAFETY REGULATIONS.

NEW SECTION. **Section 3. Admissibility of proof -- violations.** (1) Except as proof of a violation of [sections 1 through 3], evidence obtained in violation of [sections 1 through 3] is not admissible in a civil, criminal, or administrative proceeding and may not be used in any type of affidavit in an effort to obtain a search warrant or court order.

(2) The attorney general may apply for an injunction or commence a civil action against any government entity to compel compliance with the terms of [sections 1 through 3].

NEW SECTION. **Section 4. Codification instruction.** [Sections 1 through 3] are intended to be codified as an integral part of Title 46, chapter 5, part 1, and the provisions of Title 46, chapter 5, part 1, apply to [sections 1 through 3].

- END -

HOUSE BILL NO. 147

INTRODUCED BY D. ZOLNIKOV, B. BENNETT

A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING THAT A SEARCH WARRANT IS REQUIRED FOR A GOVERNMENT ENTITY TO ACCESS ANY ELECTRONIC DEVICE UNLESS INFORMED CONSENT IS OBTAINED OR A JUDICIALLY RECOGNIZED EXCEPTION TO THE WARRANT REQUIREMENT EXISTS; ~~PROVIDING THAT EVIDENCE OBTAINED IN VIOLATION IS NOT ADMISSIBLE~~ PROVIDING A CIVIL CAUSE OF ACTION FOR VIOLATIONS; AND PROVIDING DEFINITIONS AND EXCEPTIONS."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. **Section 1. Definitions.** As used in [sections 1 through 3], the following definitions apply:

(1) "AUTHORIZED USER" MEANS A PERSON WHO HAS THE PERMISSION OF THE OWNER TO POSSESS AND OPERATE THE ELECTRONIC DEVICE.

(2) "ELECTRONIC COMMUNICATION SERVICE" MEANS A SERVICE THAT:

(A) PROVIDES TO USERS THE ABILITY TO SEND OR RECEIVE ELECTRONIC COMMUNICATIONS;

(B) PROVIDES TO USERS COMPUTER STORAGE OR PROCESSING SERVICES; OR

(C) ACTS AS AN INTERMEDIARY IN THE TRANSMISSION OF ELECTRONIC COMMUNICATIONS.

~~(1)~~(3) "Electronic device" means a device that enables access to or use of an electronic communication service~~,~~ OR remote computing service~~, or location information service~~.

~~(2)~~(4) "Government entity" means a state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission or an individual acting or purporting to act for or on behalf of a state or local agency.

(5) "OWNER" MEANS A PERSON WHO IS THE LEGAL OWNER OF THE ELECTRONIC DEVICE. IF THE ELECTRONIC DEVICE IS THE SUBJECT OF AN AGREEMENT FOR THE CONDITIONAL SALE OF THE ELECTRONIC DEVICE WITH THE RIGHT OF PURCHASE UPON PERFORMANCE OF THE CONDITIONS STATED IN THE AGREEMENT AND WITH AN IMMEDIATE RIGHT OF POSSESSION VESTED IN THE PERSON POSSESSING THE DEVICE, OR IN THE EVENT THE ELECTRONIC DEVICE IS SUBJECT TO A LEASE, CONTRACT, OR OTHER LEGAL ARRANGEMENT VESTING THE RIGHT OF POSSESSION OR CONTROL IN THE PERSON POSSESSING THE ELECTRONIC DEVICE, THEN THE OWNER IS THE PERSON IN WHOM THE RIGHT OF POSSESSION

OR CONTROL IS VESTED.

~~(3)~~(6) "Remote computing service" means the provision of computer storage or processing services by means of an electronic communications system.

~~(4)~~(7) "Stored data" means data or records that are stored on an electronic device that contains:

(a) information revealing the identity of users of the applicable service, device, or program;

(b) information about a user's use of the applicable service, device, or program;

(c) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the user;

(d) the content of a wire communication or electronic communication sent to or by the user; or

(e) any data, documents, files, or communications stored by or on behalf of the user with the applicable service provider or on the user's electronic device.

NEW SECTION. **Section 2. Electronic data privacy -- warrant required -- exceptions.** (1) Except as provided in subsection (2), a government entity may not obtain the stored data of an electronic device without a search warrant issued by a court upon a finding of probable cause.

(2) A government entity may obtain the stored data of an electronic device without a search warrant:

(a) with the ~~informed, affirmative~~ consent of the owner or AUTHORIZED user of the electronic device;

(b) in accordance with judicially recognized exceptions to warrant requirements;

(c) if the owner has voluntarily and publicly disclosed the stored data;

(d) if ~~there exists a possible life-threatening situation; OR~~ THE GOVERNMENT ENTITY, IN GOOD FAITH, BELIEVES THAT AN EMERGENCY INVOLVING DANGER, DEATH, OR SERIOUS PHYSICAL INJURY TO A PERSON REQUIRES IMMEDIATE DISCLOSURE OF COMMUNICATIONS RELATING TO THE EMERGENCY;

~~(e) if a government entity has possession of a lost, stolen, or otherwise unidentified device and the government entity cannot determine ownership of the device without accessing the device, then access on the part of the government entity is limited to determining ownership and a method of contacting the owner so that the device can be returned; or~~

~~(f)~~(E) in order to respond to the user's call for emergency services; OR

(F) FOR ANY ELECTRONIC DEVICES FOUND WITHIN THE CONFINES OF AN ADULT OR YOUTH CORRECTIONAL FACILITY.

(3) Nothing in [sections 1 through 3] may be construed to limit a government entity's ability to use,

maintain, or store information on its own electronic devices or to disseminate information stored on its own electronic devices.

(4) [SECTIONS 1 THROUGH 3] DO NOT APPLY TO MOTOR CARRIER SAFETY OR HAZARDOUS MATERIALS PROGRAMS IMPLEMENTED BY THE DEPARTMENT OF TRANSPORTATION FOR PURPOSES OF COMPLYING WITH FEDERAL MOTOR CARRIER SAFETY REGULATIONS.

NEW SECTION. **Section 3. ~~Admissibility of proof -- violations~~ CIVIL ACTION FOR VIOLATION.** ~~(1) Except as proof of a violation of [sections 1 through 3], evidence obtained in violation of [sections 1 through 3] is not admissible in a civil, criminal, or administrative proceeding and may not be used in any type of affidavit in an effort to obtain a search warrant or court order.~~

~~(2)~~ The attorney general may apply for an injunction or commence a civil action against any government entity to compel compliance with the terms of [sections 1 through 3].

NEW SECTION. **Section 4. Codification instruction.** [Sections 1 through 3] are intended to be codified as an integral part of Title 46, chapter 5, part 1, and the provisions of Title 46, chapter 5, part 1, apply to [sections 1 through 3].

- END -

GOVERNOR'S OFFICE OF BUDGET AND PROGRAM PLANNING

Fiscal Note 2019 Biennium

Bill #	HB0147	**Title:**	Requiring search warrant for gov access to electronic devices
Primary Sponsor:	Zolnikov, Daniel	**Status:**	As Introduced

☐Significant Local Gov Impact ☐Needs to be included in HB 2 ☐Technical Concerns

☐Included in the Executive Budget ✓Significant Long-Term Impacts ☐Dedicated Revenue Form Attached

FISCAL SUMMARY

	FY 2018 Difference	FY 2019 Difference	FY 2020 Difference	FY 2021 Difference
Expenditures:				
General Fund	$0	$0	$0	$0
Federal Special Revenue	$0	$0	$0	$0
Revenue:				
General Fund	$0	$0	$0	$0
Federal Special Revenue	($5,000,000)	($5,000,000)	($5,000,000)	($5,000,000)
Net Impact-General Fund Balance:	$0	$0	$0	$0

Description of fiscal impact: If enacted as written, HB 147 would have a fiscal impact on federal funding for Montana Department of Transportation's Motor Carrier Services Program (MCS).

FISCAL ANALYSIS

Assumptions:

Department of Transportation

1. MCS officers and inspectors conduct Commercial Vehicle and Driver safety inspections, Motor Carrier Compliance Reviews, and Safety Audits as required by the Federal Motor Carrier Safety Administration (FMCSA) in support of the Motor Carrier Safety Assistance Program (MCSAP).
2. In order to conduct these compliance actions, inspectors and officers need to connect to an ELD (Electronic Logging Device), onboard computer, or smart phone to view driver logs, and other documentation required in FMCSA regulations.
3. If HB 147 requires officers or inspectors to obtain a warrant, MDT's non-compliance with federal grant requirements would cost approximately $5 million in grant funds annually.

	FY 2018 Difference	FY 2019 Difference	FY 2020 Difference	FY 2021 Difference
Fiscal Impact:				
FTE	0.00	0.00	0.00	0.00
Expenditures:				
Operating Expenses	$0	$0	$0	$0
Funding of Expenditures:				
General Fund (01)	$0	$0	$0	$0
Federal Special Revenue (03)	$0	$0	$0	$0
TOTAL Funding of Exp.	$0	$0	$0	$0
Revenues:				
General Fund (01)	$0	$0	$0	$0
Federal Special Revenue (03)	($5,000,000)	($5,000,000)	($5,000,000)	($5,000,000)
TOTAL Revenues	($5,000,000)	($5,000,000)	($5,000,000)	($5,000,000)
Net Impact to Fund Balance (Revenue minus Funding of Expenditures):				
General Fund (01)	$0	$0	$0	$0
Federal Special Revenue (03)	($5,000,000)	($5,000,000)	($5,000,000)	($5,000,000)

Long-Term Impacts:

1. Jeopardizing the compliance review and safety audit levels of commercial vehicles may also put MDT's federal construction funds at risk.

Sponsor's Initials	*Date*	*Budget Director's Initials*	*Date*

GOVERNOR'S OFFICE OF BUDGET AND PROGRAM PLANNING

Fiscal Note 2019 Biennium

Bill #	HB0147	**Title:**	Requiring search warrant for gov access to electronic devices
Primary Sponsor:	Zolnikov, Daniel	**Status:**	As Amended

☐Significant Local Gov Impact ☐Needs to be included in HB 2 ☐Technical Concerns

☐Included in the Executive Budget ☐Significant Long-Term Impacts ☐Dedicated Revenue Form Attached

FISCAL SUMMARY

	FY 2018 Difference	FY 2019 Difference	FY 2020 Difference	FY 2021 Difference
Expenditures:				
General Fund	$0	$0	$0	$0
Revenue:				
General Fund	$0	$0	$0	$0
Net Impact-General Fund Balance:	$0	$0	$0	$0

Description of fiscal impact: HB 147, as amended, has no fiscal impact to the state.

Sponsor's Initials *Date* *Budget Director's Initials* *Date*

The Big Sky Country

MONTANA HOUSE OF REPRESENTATIVES

SPONSOR'S REBUTTAL TO FISCAL NOTE

House Bill Number: 147 **Date Prepared:** January 10, 2017

Short Title: Requiring search warrant for gov access to electronic devices

Sponsor: Daniel Zolnikov

Generally, why do you disagree with the fiscal note?

Section 2 (2) a. allows a government entity to obtain stored data with a warrant with consent. If a driver doesn't give consent, they won't pass inspections. Compliance with an understanding of accessing data is consent.

Specifically, what in the fiscal note do you feel is flawed?

$5 million in grant funds annually is not at risk.

What is your estimate of the fiscal impact?

$0

Sponsor Signature: _____